Utah Bureau of Criminal Identification

NEWSLETTER

Department of Public Safety

VOLUME 105:4 http://bci.utah.gov JULY 2005

TAC TEST POLICY

BCI has recently changed the TAC Test policy. The TAC test will now only be required every two years, instead of every year.

Those who have taken and passed all their required tests this year will not be required to take the test in 2006. However, **you must make sure you have passed ALL of your required tests to be excused from testing in 2006.** The tests will be available to take on the UCJIS system until September 1, 2005.

Current TACs who do not pass all their required tests before September 1, 2005 will be required to test in 2006. Also, those individuals who become TACs between now and the 2006 TAC Conference will also need to take the test in 2006.

If you have any questions, please contact Jacob Dunn at (801) 965-4963.

A FEW TAC REMINDERS…

2005 TAC CONFERENCE

Thanks to everyone who attended the 2005 TAC Conference in Layton! We appreciate your questions, participation, and feedback.

A few reminders from items covered in the TAC Conference:

TACs – please run the REPT transaction on your users, and check their standing in the "Background Status" and "Criminal Record" columns. If either of these columns is blank, we will need more information on the user!

If the user is POST certified, please let us know! You can send a list of your POST certified users (names and logons) to Holly Wayman at hwayman@utah.gov.

If the user is not POST certified, we will either need that user's fingerprints, or proof that BCI ran that user's fingerprints in the past. Whenever BCI ran fingerprints in the past, we sent a letter to that user's TAC stating that we did run the prints, and the results of the background check. If you have a copy of this letter, it will serve as proof that the user's prints were sent to BCI at one point. If you do not have a copy of that letter, you will need to send in one set of applicant fingerprints for the user, along with the accompanying Fingerprint Submission form.

PASSWORDS: As mentioned at the TAC Conference, the UCCH and III passwords will be changing this week. (Watch for an e-mail or watch the Message of the Day to find out the exact date.)

Please tell your users what the new passwords are. Our Help Desk will give the new passwords only to TACs. If users call our Help Desk wanting to know the new passwords, they will be referred back to their TAC.

NEW UCJIS SYSTEM: The "old" and "new" versions of the UCJIS web page are currently available to all UCJIS users. We invite users to make themselves familiar with the "new" UCJIS program as soon as possible, before the "old" UCJIS is removed forever. Also, please contact the Help Desk or Field Services with questions or concerns about the new system. If you would like on-site training on the "new" UCJIS, please contact Jake Dunn at 801-965-4963.

REQUIRED DOCUMENTS:

Submitted your User Agreement and ORI Validation form yet? Agencies that fail to submit the 2005-2006 User Agreement may face the risk of losing their UCJIS access. Please submit these forms to Field Services as soon as possible. They may be faxed to 801-965-4749. Also, make sure you keep a copy of these documents at your agency in case they become lost at BCI, or lost on their way to BCI!

WZIP TRANSACTION & COURTS

COURTS – With the addition of the new WZIP file on UCJIS, it is more important than ever that addresses and zip codes are correctly entered on warrants.

BCI has learned that some courts are entering "default" zip codes when they don't know the real zip code of the defendant. BCI audit results have also shown that some courts do not do all they can to find, enter, and update correct addresses for defendants.

Many law enforcement agencies are giving the WZIP results to their officers so that the officers can serve the outstanding warrants. Incorrect addresses and zip codes waste valuable time and effort for these officers.

After all, if you want the person caught, let the officers know where to find the defendant!

WZIP TRANSACTION & ALL AGENCIES

Once the information from the WZIP transaction is transferred into another type of document (spreadsheet, database, word processing document, etc.) it is still considered confidential and protected information that must only be used for law enforcement purposes!

Running your own zip code, pasting the results into a spreadsheet, and passing that spreadsheet out at your neighborhood block party is just one example of blatant misuse of the WZIP transaction!

IMPORTANCE OF PASSWORD SECURITY

The following information from a recent LEO article is not only good advice for UCJIS users, but could also very well help protect you from identity theft and other problems outside of your work environment!

LEO news article June 13, 2005.

Password Security

Our computer-based world is now a maze of passwords, designed to protect our sensitive data from thieves and snoops. We mix and match birth dates, mothers' maiden names, friends, ages, addresses and nicknames in a jumble of codes for our electronic selves. But are we safe?

The folks at Fiberlink Communications Corp., a Blue Bell, PA-based maker of software and other high-tech products, conducted a recent password-cracking experiment. With an eight-character password on a standard 95-character keyboard, there are quite a few possible combinations: 6,634,204,312,890,625 to be exact, according to Fiberlink.

The company then tested a standard computer's calculative prowess against our common habit of using simple words as passcodes to protected electronic areas.

So, for the example, using the word "password" as the password, a standard desktop computer took less than a second to determine this, when assembling all the different letter combinations. Adding the single digit 1 to the password required three seconds. Typing "password" with an asterisk in the middle took the computer 38 seconds to decipher. And the combination that was not cracked, after the machine was left to compute for more than 10 minutes? p@$$w0rd

Creating Crack-Proof Passwords

Robert Stephens of the Minneapolis based Geek Squad tells us that most password-cracking programs can only crack passwords of less than fifteen characters. The longer the password, the harder it is to crack. If you want a very secure password, use the maximum number of characters a program allows. But since such a password is virtually invulnerable to cracking, be sure you know how to find it should you lose it.

To maintain the security of the LEO network, all LEO members are required to change their passwords every 90 days. If you want to create your own passwords based on the criteria set down by LEO, so be it. But in my case, I will stick with the System Generated process of random selected types of characters. And while I'm at it, I'll review all my other assorted passwords as well.

And lastly, if you share your computer with anybody, this one's pretty important. Turn off the options to auto-remember passwords so that nobody who uses your browser after you can log in to your Web sites.

Anyone having access to your passwords could pretend to be you online (a practice called "spoofing"), order products or services in your name, or invite the unwanted attention of others. Change your passwords often, and don't leave them on or near your computer. Don't select passwords that could be guessed by someone who knows you, and don't use the same password on more than one site. Combinations of eight or more alphabetic and numeric characters are your best bet when selecting a password.

Password Forgotten

Many programs will allow you to protect your documents with a password, which is meant to deter others from accessing your information. Of course, if you forget your own password, you can't get in there, either. In the case of LEO you simply contact the Technical Support Center at 888-334-4536, 24 hours per day, 7 days per week, and they can walk you through a verification process.

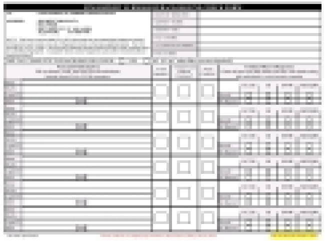
In the case of other programs, you may have to hike down to your local computer repair shop, or contact the company that wrote the software program you're using and deal with their tech service. In either case, it is probably going to cost you valuable time and/or money. In some cases, if you enter an improper password several times, a prompt screen will pop up allowing you to walk through a verification process.

As a last resort, there is a variety commercial cracking programs readily available for purchase over the Internet, as well as plenty of free cracking programs on freeware/shareware or hacker Web sites. Although I do not recommend this last option, URLs can be located as close as your favorite search engine.

TIPS 4 TACS

Law enforcement applicant fingerprints must not be submitted to BCI without the accompanying "Background Check Request Form." Also, the "Background Check Request Form" must not be sent to BCI without fingerprints (unless the user is POST certified, and has no criminal history.)

If BCI receives the "Background Check Request Form" without the necessary fingerprints, the form is shredded, and the agency is *not* notified.



UCR/IBR

City/County Attorneys and UCR/IBR Submission:

There are some questions that your agency must address before you can start submitting Uniform Crime Reports:

1) Does your office have sworn POST Certified law enforcement officers with arrest powers?

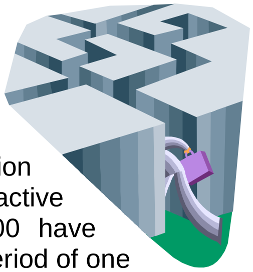
2) Does your agency initiate the crime report? Or, do you get the your report from a law enforcement agency, investigate and/or prosecute these criminal cases?

If you can answer yes to both questions, BCI wants to help you get started with UCR submissions. And, if you qualify as a UCR participant, we need to assign you a law enforcement ORI for UCR purposes only.

MISSING PERSONS

MISSING ADULTS

HOW CAN PEOPLE JUST DISAPPEAR?



Many families ask themselves that question. As of March 21, 2005 there were approximately 47,663 active missing person's cases in the National Crime Information Center (NCIC). Of those active cases in NCIC nearly 30,000 have remained missing for over a period of one year.

There are varying reasons an individual goes missing, whether voluntarily or involuntarily and the complexities of investigating an adult case. Understanding those contributors is key to changing the way missing person cases are responded to by the public and the law enforcement community. As adults we have a right to go missing if we so choose. We can pick up and leave at any time, never contact our families and start a new life. That is our right as adults. However, this is commonly the first assumption that is made when an adult, over the age of eighteen, vanishes. Yet, in many cases families may never know what happened and are left with only hope that their loved one is alive.

Many of us are affected by family members suffering from Alzheimer's disease or other health or lifestyle related issues. When an individual vanishes law enforcement agencies have the difficult task of determining if the missing adult is at risk by establishing whether the individual has a diminished mental capacity, a physical disability, a need for medication, is suffering from substance abuse, domestic violence, financial woes or other factors that may not always be clear. When foul play is involved in an individual's disappearance every hour that passes makes it even more difficult to make that determination. Missing persons are our sons, our daughters, mothers, fathers or even our grand-parents and we need to ask ourselves, "Could this could happen in our own family?" Sadly, the answer is yes!

Missing Adults And NCIC Entries

When an agency enters a missing adult into NCIC, that record should remain in the system until the missing person is located. When a record is removed from the system before the person is located there is a chance that an unidentified body in a surrounding state could never be identified. There are currently 5,814 active unidentified records into NCIC. When initially entered or modified, NCIC uses algorithms to automatically compare Missing and Unidentified records against each other and notifies agencies of possible hits. This program is run once a day. If you have questions on missing or unidentified records you can contact Gina McMahon at (801) 965-4686 or gmcmahon@utah.gov

PRESIDENT'S DNA INITIATIVE FOR MISSING/UNIDENTIFIED

Each day in the United States there are nearly 100,000 active missing persons cases, many of these reported years ago. Of these missing person cases almost 50,000 are individuals over the age of eighteen. Experts have estimated there are nearly 40,000 unidentified remains that have not been properly recorded by law enforcement agencies and medical examiners nationwide.

The process of identifying unidentified or missing persons has become a monumental challenge for law enforcement. In the past, identification was made possible by gathering data from the location the missing person was last seen, crime scenes and other sources, and comparing dental and medical records. All remain challenging methods of identification. With the advancement of technology and the discovery of the genetic records stored within the DNA of the human body, DNA identification has become the most viable means of making close to 99% accurate identification.

Recognizing the importance of DNA testing for the identification of missing and unidentified persons, and assessing the financial needs of forensic investigators, President Bush announced a DNA Initiative in 2003. This initiative authorized the Attorney General to use designated funds specifically for DNA identification to ensure DNA technology is used to its full potential in identifying missing persons and unidentified dead.

The process of DNA identification is performed in two ways, one being nuclear and the other mitochondrial DNA testing. Currently the University of North Texas Health and Science Center (UNTHSC) is one of two facilities in the nation that have the capability of uploading mitochondrial DNA into the Federal Bureau of Investigation (FBI) Combined DNA Index System (CODIS).

In 2003 the University of North Texas Health and Science Center established the Texas Missing Persons DNA Database and was tasked with the development, procurement, and distribution of sample collection kits. This effort has now been expanded to include the development of two standardized collection kits. One kit provides a safe and effective, non-invasive means for collecting family reference samples. The second kit has been developed for the collection, transportation and storage of human remains. UNTHSC will be working in conjunction with the FBI Laboratory, International Homicide Investigators Association (IHIA), National Association of Medical Examiners (NAME), the National Center for Missing & Exploited Children (NCMEC) and the National Center for Missing Adults (NCMA) to ensure proper utilization of the collection kits. For more information you can go to www.dna.gov